

## TOP 3 SCHOOL SECURITY MISTAKES

# 1 FAILURE TO RECEIVE AN INDEPENDENT EXPERT ASSESSMENT OF YOUR SAFETY AND SECURITY

The first mistake many schools make is to believe that self-assessments, or an assessment done by a local law enforcement officer, are sufficient to comprehensively evaluate their safety and security. Self-assessments and those done by law enforcement have value. But they also have shortcomings from potential bias, blind spots (don't know what they don't know), and a lack of objectivity. They are a good first step. But they are not a substitute for an independent assessment by someone outside your organization and the narrow background of law enforcement who is familiar with the full breadth of school safety and security best practices and available tools, and identifying related vulnerabilities in your unique schools.

**Effective assessment is a two-part process:** a self-assessment followed by an independent assessment is the best method to ensure the most objective and comprehensive identification of safety and security threats. Its purpose is to provide the *foundation* for your district to develop and implement effective plans to eliminate or mitigate those safety vulnerabilities.

Your Staff training should also not be generic; it should be guided by the findings from the two-part assessment process.

A comprehensive Threat, Vulnerability, and Risk Assessment of each facility should include all of the following:

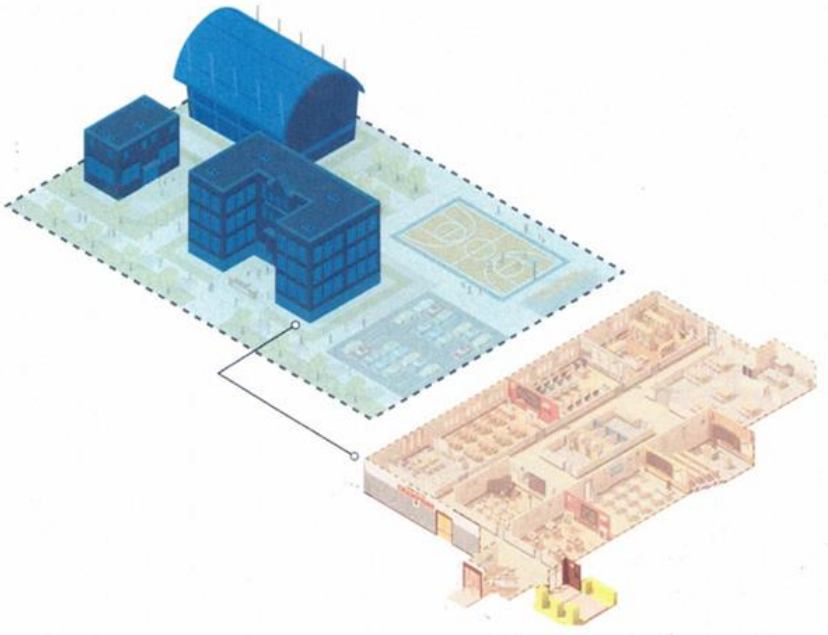


## TOP 3 SCHOOL SECURITY MISTAKES

## 2 NOT FOCUSING ON ALL LAYERS OF SAFETY AND SECURITY – HARDWARE IS NOT A PANACEA

School safety and security occurs in layers. These layers include four separate physical security layers, but also includes emergency planning, training, and necessary supplies.

The four school physical security layers are illustrated below:

- 
- The diagram illustrates the four layers of school physical security. It shows a school campus with buildings, a parking lot, and a playground. The layers are represented by different colors and patterns: a dashed line for the grounds perimeter, a light blue area for the school grounds, a dark blue area for the building perimeter, and a tan area for the building interior. A legend on the left lists the layers with corresponding icons.
1. The **grounds perimeter layer**, which demarcates the outer boundary of a school campus;
  2. The **school grounds layer**, which encompasses athletic fields, parking lots, playgrounds, and any other outdoor space that is part of a school's campus;
  3. The **building perimeter layer**, or walls enclosing the inside of school buildings; and
  4. The **building interior layer**, which comprises all of the spaces inside school buildings (e.g. administrative offices, hallways, cafeterias, classrooms, gymnasiums, auditoriums, etc.).

Schools are cautioned against focusing their resources on physical security and related hardware to the exclusion of adequate emphasis on good planning and training for potential emergency events. For example, use of security cameras. Those can be very important pieces of an overall plan but, alone, they often do not prevent or assist in responding to a threat. Security cameras that are not monitored in real time but are used only for after-the-fact video purposes will provide a limited impact on security. Effective school safety and security is a product of creating multiple layers in a comprehensive safety and security program. And that includes more emphasis on the human element: staff training.

## TOP 3 SCHOOL SECURITY MISTAKES

### 3 FAILURE TO TRAIN PEOPLE ENOUGH

Failing to effectively train people on emergency response is a major shortcoming that can negate even the most advanced safety and security technology and equipment. ***The best equipment and best written EOP will fail unless the people responsible to take action do so when and if an emergency event happens.*** Decades of social science establishes that people faced with a crisis tend to respond with hardwired responses (fight, flight, freeze). But those responses are unpredictable and vary from person to person. Worse, they may be precisely the wrong response to a particular emergency event. How is that avoided? Training, training, and more training. Social science also shows that sufficient training results in trained responses to crisis situations. Good illustrations of this principle exist in military, law enforcement, emergency medicine, and first responders.

Training must be repeated. It is perishable. Fact: people who train frequently are much more likely to successfully respond to a crisis incident.

SSC recommends the following regarding training.

- a. Training should not be limited to only active shooter response. For example, a cardiac emergency including use of AEDs and CPR. Those events happen far more frequently.
- b. Training should be given to everyone in the organization who may need to respond to a crisis event, not just selected staff. Teaching and non-teaching staff. And Students.
- c. Training is not generic one-size-fits-all. It should be custom to *your* school and operations. Therefore, training should always follow an assessment. A security consultant who does not know *your* operations or environment can't really train you how to respond to an emergency in *your* environment.
- d. Training is perishable and should be done regularly. People forget. Your staff has turnover. Best practices change over time. Your facilities and technology change over time. All these realities call for fresh training.